นโยบายคลาวด์และการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ระหว่างสหภาพยุโรป สหรัฐอเมริกา ออสเตรเลีย และอาเซียน : มุมมองของไทย

สราวุธ ปิติยาศักดิ์*

Received: December 20, 2017
Revised: October 29, 2018
Accepted: November 20, 2018

บทคัดย่อ

การศึกษาวิจัยนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาแนวคิดและทฤษฎีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล 2) เปรียบเทียบนโยบายคลาวด์และกฎหมายคุ้มครองข้อมูลส่วนบุคคลระหว่างประเทศต่าง ๆ และ 3) ศึกษาปัญหาและอุปสรรคเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ในประเทศไทย โดยศึกษาข้อมูลเอกสาร สัมภาษณ์เชิงลึกผู้เชี่ยวชาญเกี่ยวกับคลาวด์และการคุ้มครองข้อมูลส่วนบุคคลรวม 10 ท่าน และสนทนากลุ่มภาคราชการ ภาคเอกชน ภาควิชาการและภาคประชาสังคม 20 ท่าน ผลการศึกษาวิเคราะห์พบว่า 1) ทุกประเทศในกลุ่มประเทศโออีซีดีและสหภาพยุโรปมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล 2) ประเทศส่วนใหญ่ในกลุ่มประเทศเอเปกมีกฎหมายคุ้มครองข้อมูลส่วนบุคคล นโยบายของรัฐบาลมีส่วนสำคัญในการสนับสนุนการใช้งานคลาวด์ และ 3) การขยายหลักดินแดนของกฎข้อบังคับของสหภาพยุโรปมีผลกระทบต่อผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (ผู้ให้บริการคลาวด์) นอกสหภาพยุโรปที่ประมวลผลข้อมูลส่วนบุคคลของบุคคลในสหภาพยุโรป ฉะนั้น กฎหมายที่บังคับใช้เฉพาะผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่ในประเทศไทยจึงไม่เพียงพอกับการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ การวิจัยนี้จึงเสนอให้ไทยจัดทำกรอบธรรมาภิบาลของข้อมูลและจำแนกข้อมูลออกเป็นประเภทอย่างชัดเจนเพื่อการจัดการและการใช้ข้อมูลแต่ละประเภทในระบบคลาวด์อย่างเหมาะสม เร่งรัดบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคล และ

* น.บ. (นิติศาสตรบัณฑิต) (เกียรตินิยมอันดับหนึ่ง), บธ.บ. (บริหารธุรกิจบัณฑิต), LL.M (Master of Law), SJD. (Doctor of Legal Science), University of Hong Kong, Hong Kong SAR, China. รองศาสตราจารย์ประจำสาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช

ขยายขอบเขตบังคับใช้กฎหมายแก่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกประเทศไทยซึ่งได้เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลภายในประเทศไทยไว้ในร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล

คำสำคัญ : นโยบายคลาวด์ การคุ้มครองข้อมูลส่วนบุคคล ขอบเขตบังคับใช้กฎหมาย

ผู้รับผิดชอบบทความ : รศ.ดร.สราวุธ ปิติยาศักดิ์ สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช 9/9 หมู่ 9 ตำบลบางพูด อำเภอปากเกร็ด จังหวัดนนทบุรี 11120 โทรศัพท์ 08 6606 2002 E-mail : spitiyas@hotmail.com

Cloud Computing Policy and Personal Data Protection in the Cloud among the European Union, the United States, Australia and ASEAN : A Thailand Perspective

Saravuth Pitiyasak*

Abstract

The purposes of this research were: 1) to study concepts and theories related to personal data protection; 2) to compare cloud computing policy and personal data protection laws among various countries; and 3) to examine problems and difficulties concerning Thailand's data protection in the cloud. The methodology employed documentary research, analysis of interviews with 10 cloud computing and data protection experts, and group discussion with 20 stakeholders from government, private, academic and community sectors. Analyzes showed that; 1) all member countries of OECD and EU had enacted the data protection laws; 2) most APEC member countries had passed the data protections laws. Government policy, meanwhile, played an important role in the adoption of cloud computing; and 3) the General Data Protection Regulation's extraterritorial scope had implications for personal data controllers and for personal data processors (cloud service providers) outside of the EU that were processing the personal data of EU residents. Thus, the current draft data protection law, applicable only to personal data controllers domiciled or located within Thailand was not sufficient for protecting personal data in the cloud. This finding suggested that Thailand should set up a data governance framework and classified data into discrete categories for the appropriate management and use of classified data stored in the cloud. The enactment of its personal data protection law and expanded its legal scope accelerated to enforce its personal data protection law

* SJD. (Doctor of Legal Science), Associate professor School of Law, Sukhothai Thammathirat Open University

for personal data controllers and personal data processors domiciled or located outside of Thailand who were collecting, using, or disclosing personal data within Thailand.

Key Words : Cloud computing, Personal data protection, Legal scope

Corresponding Author : Assoc.Prof. Saravuth Pitiyasak, School of Law, Sukhothai Thammathirat Open University, 9/9 Moo 9 Chaengwattana Rd. Bangpood, Pakkret Nonthaburi 11120. Tel 08 7049 8486 E-mail : spitiyas@hotmail.com

บทนำ

คลาวด์คอมพิวติง (cloud computing) เป็นการให้บริการทรัพยากรทางคอมพิวเตอร์ เช่น หน่วยความจำ หน่วยจัดเก็บข้อมูล ซอฟต์แวร์ในการประมวลผลข้อมูลและเครือข่าย เป็นต้น โดยผู้ใช้บริการสามารถเพิ่มและลดทรัพยากรทางคอมพิวเตอร์เหล่านี้ได้ตามความต้องการ ส่งผลให้เกิดความสะดวกรวดเร็วในการใช้งานและประหยัดค่าใช้จ่าย ทำให้ระบบคลาวด์ได้รับความนิยมจากผู้ใช้บริการเป็นจำนวนมากขึ้นทุกวัน โดยเฉพาะอย่างยิ่งการเพิ่มขึ้นอย่างรวดเร็วของพาณิชย์อิเล็กทรอนิกส์ ยิ่งทวีความต้องการในการใช้บริการระบบคลาวด์เพื่อการประมวลผลข้อมูล รวมถึงการส่งหรือโอนข้อมูลข้ามพรมแดนระหว่างประเทศเพิ่มมากขึ้น

ในสหภาพยุโรป ระบบคลาวด์มีบทบาทสำคัญในการบรรลุกลยุทธ์ตลาดดิจิทัลเดียวของสหภาพยุโรป (EU Digital Single Market Strategy) ทำให้เกิดการไหลเวียนของข้อมูลอย่างอิสระ (free flow of data) อันเป็นหลอดเลือดใหญ่ของกลยุทธ์ตลาดดิจิทัลเดียว อย่างไรก็ดี การใช้บริการคลาวด์คอมพิวติงอาจก่อให้เกิดปัญหาความเสี่ยงต่อความปลอดภัยของข้อมูล โดยเฉพาะอย่างยิ่งเมื่อข้อมูลส่วนบุคคลซึ่งได้ถูกอัปโหลด (upload) เข้าไปอยู่ในระบบคลาวด์ แล้วมีการส่งหรือโอนไปยังประเทศที่สามนอกสหภาพยุโรป ปัญหาความเสี่ยงต่อความปลอดภัยของข้อมูลส่วนบุคคลดังกล่าวนำไปสู่ประเด็นทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ ดังนั้น เมื่อวันที่ 25 มกราคม พ.ศ. 2555 คณะกรรมาธิการยุโรปด้านการยุติธรรมได้เสนอให้มีการปรับปรุงกฎระเบียบคุ้มครองข้อมูลส่วนบุคคลแห่งสหภาพยุโรปที่ 95/46/EC (Directive 95/46/EC) ต่อคณะมนตรีและรัฐสภายุโรป ซึ่งต่อมาในวันที่ 27 เมษายน พ.ศ. 2559 คณะมนตรีและรัฐสภายุโรปได้ออกกฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลแห่งสหภาพยุโรปที่ 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data or General Data Protection Regulation : GDPR) โดยมีผลบังคับใช้ในวันที่ 25 พฤษภาคม พ.ศ. 2561 และเมื่อกฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลแห่งสหภาพยุโรปมีผลบังคับใช้ กฎระเบียบคุ้มครองข้อมูลส่วนบุคคลแห่งสหภาพยุโรปที่ 95/46/EC จะถูกยกเลิกไปในทันที

กฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปได้ปรับเปลี่ยนโครงสร้าง ขยายขอบเขตการบังคับใช้ และแก้ไขเพิ่มเติมเนื้อหาและกลไกบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรปอย่างมีนัยสำคัญหลายประการ ได้แก่

ประการแรก กฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปได้เปลี่ยนแปลงโครงสร้างของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรป กล่าวคือ กฎข้อบังคับได้เปลี่ยนแปลงโครงสร้างของกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้เป็นหนึ่งเดียวกันทั้งสหภาพยุโรป โดยการเปลี่ยนจาก “กฎระเบียบ (Directive)” ซึ่งเป็นเพียงแนวทางให้แต่ละประเทศสมาชิกสหภาพยุโรปนำไปออกกฎหมายภายในประเทศของตน ไปเป็น “กฎข้อบังคับ (Regulation)” ซึ่งมีผลบังคับใช้เสมือนหนึ่งกฎหมายภายในของทุกประเทศสมาชิกสหภาพยุโรป ทำให้ทุกประเทศสมาชิกของสหภาพยุโรปมี

กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เหมือนกันเป็นหนึ่งเดียว ส่งผลให้ธุรกิจในสหภาพยุโรปสามารถลดค่าใช้จ่ายในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพราะการปฏิบัติตามกฎข้อบังคับฉบับเดียวสามารถใช้ได้ทั้งสหภาพยุโรป จากเดิมที่ต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศสมาชิกของสหภาพยุโรปที่องค์กรเข้าไปประกอบธุรกิจ

ประการที่สอง กฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปได้ขยายขอบเขตบังคับใช้ของกฎข้อบังคับออกไปยังผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลนอกสหภาพยุโรป กล่าวคือ นอกจากกฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปจะบังคับใช้กับธุรกิจในสหภาพยุโรป หรือธุรกิจจากประเทศที่สามที่เข้ามาลงทุนตั้งสำนักงานในสหภาพยุโรปซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแล้ว กฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป มาตรา 3(2) ยังบังคับใช้กับธุรกิจในประเทศที่สามซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกสหภาพยุโรป แต่ได้เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลส่วนบุคคลในสหภาพยุโรปหรือมีการติดตามตรวจสอบพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในสหภาพยุโรป

ประการสุดท้าย กฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป มาตรา 83(4) ได้กำหนดกลไกการบังคับใช้กฎหมายที่เข้มงวดขึ้น โดยได้กำหนดเพิ่มค่าปรับทางปกครองแก่ธุรกิจที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตามกฎข้อบังคับสูงถึง 10 ล้านยูโร หรือร้อยละ 2 ของรายได้ (ต่อปี) จากการดำเนินงานทั่วโลก ในกรณีที่ไม่ปฏิบัติตามหน้าที่ที่กฎข้อบังคับกำหนดไว้ และมาตรา 83(4) กำหนดค่าปรับ 20 ล้านยูโร หรือร้อยละ 4 ของรายได้ (ต่อปี) จากการดำเนินงานทั่วโลก ในกรณีละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคล ส่งหรือโอนข้อมูลส่วนบุคคลออกนอกสหภาพยุโรปโดยฝ่าฝืนหรือละเมิดกฎข้อบังคับ

จากการปรับเปลี่ยนข้างต้น จึงเห็นได้ว่านโยบายคลาวด์และกฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปมีผลกระทบต่อธุรกิจนอกสหภาพยุโรปอย่างมีนัยสำคัญ เพราะมีทั้งการขยายหลักดินแดนคุ้มครองข้อมูลส่วนบุคคลและการเพิ่มมาตรการการลงโทษที่เป็นค่าปรับจำนวนมาก ซึ่งเมื่อกฎข้อบังคับฉบับนี้มีผลบังคับใช้ในวันที่ 25 พฤษภาคม พ.ศ. 2561 ประเทศไทยซึ่งเป็นคู่ค้าหนึ่งของประเทศในสหภาพยุโรป จำต้องศึกษาและพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยเพื่อให้พร้อมรับมือกับผลกระทบของกฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปดังกล่าว

วัตถุประสงค์

1. เพื่อศึกษาแนวคิดและทฤษฎีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

2. เพื่อเปรียบเทียบนโยบายคลาวด์และกฎหมายคุ้มครองข้อมูลส่วนบุคคลระหว่างประเทศต่าง ๆ

3. เพื่อศึกษาปัญหาและอุปสรรคเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ในประเทศไทย

วิธีวิจัย

1. ศึกษาข้อมูลเอกสาร ได้แก่ ตัวบทกฎหมาย คำพิพากษา ตำรา หนังสือ บทความ วิทยานิพนธ์ สารนิพนธ์ วิจัย และสื่ออิเล็กทรอนิกส์อื่น ๆ ใน

ประเด็นที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งในระบบคลาวด์ทั้งภาษาไทยและต่างประเทศ

2. ศึกษาข้อมูลเกี่ยวกับปัญหาและอุปสรรคเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ในประเทศไทย โดยวิธีการ

2.1 สัมภาษณ์เชิงลึกกลุ่มผู้เชี่ยวชาญที่เกี่ยวข้องกับคลาวด์และการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ทั้งทางด้านเทคโนโลยีและทางด้านกฎหมาย 10 ท่าน ได้แก่ 1) กรรมการร่างรัฐธรรมนูญ พ.ศ. 2560 2) ผู้อำนวยการสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) 3) กรรมการผู้จัดการบริษัทอินเทอร์ลิ้งค์ คอมมิวนิเคชั่น จำกัด (มหาชน) 4) กรรมการผู้จัดการบริษัทอินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) 5) กรรมการผู้จัดการบริษัท ที-เน็ต จำกัด 6) ที่ปรึกษาด้านความมั่นคงปลอดภัยไซเบอร์ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ 7) นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม 8) อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 9) อาจารย์ประจำคณะวิทยาการสารสนเทศ มหาวิทยาลัยบูรพา และ 10) ผู้ประสานงานเครือข่ายพลเมืองเน็ต

2.2 จัดการสนทนากลุ่ม (focus group discussion) ประกอบด้วย ภาคราชการ ภาคเอกชน ภาควิชาการ และภาคประชาสังคม 20 ท่าน ได้แก่ 1) กรรมการร่างรัฐธรรมนูญ พ.ศ. 2560 2) ที่ปรึกษาปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม 3) รองผู้อำนวยการสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) 4) ที่ปรึกษาด้านความมั่นคงปลอดภัยไซเบอร์สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ 5) ผู้อำนวยด้านกฎหมายคณะกรรมการร่วมภาคเอกชน 3 สถาบัน (กกร.) 6) ตัวแทนสมาคมธนาคารไทย (ฝ่ายกฎหมายธนาคารกรุงเทพ จำกัด (มหาชน)) 7)ผู้แทนสำนักงานประกันสุขภาพแห่งชาติ (สปสช.) 8) หัวหน้าห้องปฏิบัติงานการวิจัยความมั่นคงปลอดภัยไซเบอร์ สำนักงานวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) 9) นิติกรปฏิบัติการระดับสูง สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) 10) นิติกรปฏิบัติการระดับต้น สำนักงาน กสทช. 11) ผู้อำนวยการสายทรัพยากรบุคคลและบริหารทั่วไป บริษัทการบินไทย จำกัด (มหาชน) 12) ทนายความและกรรมการสมาคมอีเลิร์นนิ่งแห่งประเทศไทย 13) อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ 14) อาจารย์ประจำคณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์ 15) อาจารย์ประจำคณะนิติศาสตร์ มหาวิทยาลัยบูรพา 16) ผู้ประสานงานเครือข่ายพลเมืองเน็ต 17) ผู้อำนวยการกองกฎหมาย สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม 18) นิติกรชำนาญการพิเศษ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม 19) นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และ 20) นักวิชาการคอมพิวเตอร์ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ผลการศึกษา

1. แนวคิดและทฤษฎีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์

จากการศึกษาจากข้อมูลเอกสารพบว่า

1) กลุ่มประเทศภายในองค์การเพื่อความร่วมมือและการพัฒนาทางเศรษฐกิจหรือโออีซีดี (Organisation for Economic Co-operation and Development; OECD) มีสมาชิกจำนวน 35 ประเทศ ประกอบด้วย ออสเตรเลีย ออสเตรีย เบลเยียม แคนาดา ชิลี สาธารณรัฐเช็ก เดนมาร์ก เอสโทเนีย ฟินแลนด์ ฝรั่งเศส เยอรมนี กรีซ ฮังการี ไอซ์แลนด์ ไอร์แลนด์ อิสราเอล อิตาลี ญี่ปุ่น เกาหลีใต้ เลทเวีย ลักเซมเบิร์ก เม็กซิโก เนเธอร์แลนด์ นิวซีแลนด์ นอร์เวย์ โปแลนด์ โปรตุเกส สาธารณรัฐสโลวัก สโลเวียเนีย สเปน สวีเดน สวิตเซอร์แลนด์ ตุรกี สหราชอาณาจักร และสหรัฐอเมริกา โดย 34 ประเทศบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นลักษณะกฎหมายทั่วไป (comprehensive law) เว้นสหรัฐอเมริกาที่บัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นลักษณะกฎหมายเฉพาะภาคส่วน (sectoral laws)

2) กลุ่มประเทศภายในความร่วมมือทางเศรษฐกิจเอเชีย-แปซิฟิก หรือเอเปก (Asia-Pacific Economic Cooperation; APEC) พบว่า เอเปกมีสมาชิกทั้งสิ้น 20 ประเทศกับ 1 เขตปกครองพิเศษ ประกอบด้วย ออสเตรเลีย แคนาดา สาธารณรัฐประชาชนจีน เขตปกครองพิเศษฮ่องกง (ส่วนหนึ่งของสาธารณรัฐประชาชนจีน) ญี่ปุ่น เกาหลีใต้ มาเลเซีย เม็กซิโก นิวซีแลนด์ เปรู ฟิลิปปินส์ รัสเซีย สิงคโปร์ ไต้หวัน สหรัฐอเมริกา ชิลี ปาปัวนิวกินี อินโดนีเซีย เวียดนาม บรูไน และไทย โดยในกลุ่มประเทศเอเปก มีเพียง 6 ประเทศเท่านั้นที่ยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป ได้แก่ ชิลี อินโดนีเซีย ปาปัวนิวกินี เวียดนาม บรูไน และไทย

3) สหภาพยุโรปมีสมาชิกทั้งสิ้น 28 ประเทศ ประกอบด้วย ออสเตรีย เบลเยียม บัลแกเรีย โครเอเชีย ไซปรัส สาธารณรัฐเช็ก เดนมาร์ก เอสโตเนีย ฟินแลนด์ ฝรั่งเศส เยอรมนี กรีซ ฮังการี ไอร์แลนด์ อิตาลี ลัตเวีย ลิทัวเนีย มอลตา ลักเซมเบิร์ก เนเธอร์แลนด์ โปแลนด์ โปรตุเกส โรมาเนีย สเปน สโลวีเนีย สโลวาเกีย สวีเดน และสหราชอาณาจักร ซึ่งหลังจากวันที่ 25 พฤษภาคม พ.ศ. 2561 จะอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับเดียวกันคือ กฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป

ในด้านการให้บริการคลาวด์ พ.ศ. 2559 ทั่วโลกมีมูลค่าประมาณ 210,000 ล้านเหรียญสหรัฐ และมีการคาดการณ์ว่า มูลค่าจะได้เพิ่มขึ้นเป็น 246,000 ล้านเหรียญสหรัฐใน พ.ศ. 2560 และเพิ่มเป็น 383,000 ล้านเหรียญสหรัฐใน พ.ศ. 2563 ซึ่งเป็นการเพิ่มขึ้นอย่างต่อเนื่อง (Gartner Inc., 2017) โดยสมาคมคลาวด์แห่งเอเชีย (Asia Cloud Computing Association, 2018) ได้จัดอันดับความพร้อมในด้านคลาวด์ใน ค.ศ. 2018 ให้สิงคโปร์ มาเลเซีย ฟิลิปปินส์ ไทย อินโดนีเซีย และเวียดนาม ได้อันดับ 1 อันดับ 8 อับดับ 9 อันดับ 10 อันดับ 11 และอันดับ 14 ตามลำดับ โดยปัจจัยสำคัญที่ใช้ในการจัดอันดับมี 4 ประการคือ 1) โครงสร้างพื้นฐานระบบคลาวด์ (cloud infrastructure) 2) ความปลอดภัยระบบคลาวด์ (cloud security) 3) กฎข้อบังคับควบคุมระบบคลาวด์ (cloud regulation) และ 4) ธรรมาภิบาลระบบคลาวด์ (cloud governance)

2. นโยบายคลาวด์และกฎหมายคุ้มครองข้อมูลส่วนบุคคลระหว่างประเทศต่าง ๆ

ผู้วิจัยได้ทำการศึกษาเปรียบเทียบนโยบายคลาวด์และการคุ้มครองข้อมูลส่วนบุคคลระหว่างสหภาพยุโรป สหรัฐอเมริกา ออสเตรเลีย สิงคโปร์ มาเลเซีย ฟิลิปปินส์ และไทย ใน 2 ประเด็นหลักที่สำคัญคือ นโยบายคลาวด์กับความมั่นคงปลอดภัยในระบบคลาวด์ และกฎหมายคุ้มครองข้อมูลส่วนบุคคลกับการขยายขอบเขตการบังคับใช้กฎหมาย รวมทั้งประเด็นย่อยที่เกี่ยวข้องอีก 3 ประเด็น โดยได้ทำเป็นตารางเปรียบเทียบไว้ดังนี้

1) นโยบายคลาวด์กับความมั่นคงปลอดภัยในระบบคลาวด์

สหภาพยุโรป	● พ.ศ. 2558 คณะกรรมาธิการแห่งสหภาพยุโรปได้กำหนดกลยุทธ์ตลาดดิจิทัลเดียวขึ้น โดยมีความเห็นว่ากลยุทธ์ตลาดดิจิทัลเดียวต้องถูกสร้างขึ้นบนระบบคลาวด์ จึงได้ออกเอกสารเชิงนโยบายที่เกี่ยวกับตลาดดิจิทัลเดียวจำนวน 2 ฉบับคือ เอกสารเชิงนโยบายฉบับแรกเกี่ยวข้องกับโครงการริเริ่มคลาวด์ยุโรป และเอกสารเชิงนโยบายเกี่ยวกับกลยุทธ์สำหรับมาตรฐาน (European Commission, 2015)
สหรัฐอเมริกา	● พ.ศ. 2553 สหรัฐอเมริกาเผยแพร่ ‘แผนการ 25 ข้อในการปรับปรุงการจัดการเทคโนโลยีสารสนเทศของรัฐบาลกลาง’ โดยแผนการย่อยข้อที่สามของแผนการดังกล่าว ได้แก่ นโยบายคลาวด์เฟิร์ส และ พ.ศ. 2554 ได้เผยแพร่กลยุทธ์คลาวด์คอมพิวติงของรัฐบาลกลาง (Vivek Kundra, 2011)
ออสเตรเลีย	● พ.ศ. 2557 รัฐบาลเครือรัฐออสเตรเลียได้ประกาศนโยบายคลาวด์เฟิร์สและกำหนดให้กิจการของเครือรัฐออสเตรเลียที่ไม่ได้แยกเป็นนิติบุคคล (NCE) ต้องใช้คลาวด์คอมพิวติงทั้งสำหรับงานทางด้านไอซีทีใหม่และทดแทนระบบเดิม (Australian Government, Department of Finance, 2014)
สิงคโปร์	● สิงคโปร์เป็นศูนย์กลางให้บริการคลาวด์ที่สำคัญแห่งหนึ่งในภูมิภาคเอเชีย-แปซิฟิก (APEC) โดยบริษัทสิงเทล (Singapore Telecommunications Limited: SingTel) ได้จัดทำโครงสร้าง G-Cloud ซึ่งเป็นคลาวด์ส่วนตัว (private cloud) สำหรับรัฐบาลสิงคโปร์และหน่วยงานของรัฐบาลขึ้นใน พ.ศ. 2556 (Infocomm Media Development Authority of Singapore, 2017)
มาเลเซีย	● พ.ศ. 2556 ศูนย์การพัฒนามัลติมีเดียมาเลเซีย (MDEC) ได้จัดทำโครงการริเริ่มคลาวด์มาเลเซีย (MSC Malaysia Cloud Initiative) ขึ้น โดยมีวัตถุประสงค์เพื่อสร้างบรรยากาศที่สนับสนุนการใช้คลาวด์คอมพิวติงขึ้นในมาเลเซียทั้งในด้านอุปสงค์และอุปทาน (Malaysia Digital Economic Corporation, 2017) โดยวันที่ 19 ตุลาคม พ.ศ. 2560 ศูนย์การพัฒนามัลติมีเดียมาเลเซียมีแผนนำกลยุทธ์คลาวด์เฟิร์ส (Cloud first Strategy) มาใช้เพื่อพัฒนากรอบปัญญาประดิษฐ์แห่งชาติ (National AI Framework) (Sainul Abudheen 2017)
ฟิลิปปินส์	● วันที่ 17 มกราคม พ.ศ. 2560 รัฐบาลฟิลิปปินส์ประกาศนโยบายคลาวด์เฟิร์สให้ทุกกระทรวง กรม สำนักงานและหน่วยงานอื่นของรัฐบาล รวมทั้งคณะกรรมาธิการตามรัฐธรรมนูญ รัฐสภา ศาลยุติธรรม สำนักงานผู้ตรวจการแผ่นดิน มหาวิทยาลัยและวิทยาลัยของรัฐ บริษัทที่รัฐบาลเป็นเจ้าของและมีอำนาจควบคุม และหน่วยงานรัฐบาลท้องถิ่นทั้งหมดนำคลาวด์มาใช้ (Republic of Philippines, Department of Information and Communications Technology, 2017)
ไทย	● สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) หรือ อีจีเอ (Electronic Government Agency : EGA) เป็นผู้มีหน้าที่รับผิดชอบพัฒนาระบบคลาวด์ภาครัฐ (Government Cloud : G-Cloud) ซึ่งเป็นโครงสร้างพื้นฐานบนอินเทอร์เน็ตแบบใช้ทรัพยากรร่วมกัน ให้บริการแก่หน่วยงานภาครัฐในการเก็บทรัพยากรทางด้านสารสนเทศไว้บนอินเทอร์เน็ต

2) กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับการขยายขอบเขตการบังคับใช้กฎหมาย

สหภาพยุโรป	● กฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (The General Data Protection Regulation; GDPR) มาตรา 3(2) เป็นการบังคับใช้กฎข้อบังคับโดยการขยายหลักดินแดน (Extraterritorial scope) ซึ่งใช้กับการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลที่อยู่ในสหภาพยุโรปโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ไม่มีสถานประกอบการตั้งอยู่ในสหภาพยุโรป แต่กิจกรรมการประมวลผลข้อมูลส่วนบุคคลนั้นเกี่ยวกับกรณีใดกรณีหนึ่งดังต่อไปนี้ (ก) การเสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลส่วนบุคคลในสหภาพยุโรป โดยไม่ต้องคำนึงถึงว่า การชำระเงินของเจ้าของข้อมูลส่วนบุคคลดังกล่าวจะเกิดขึ้นในสหภาพยุโรปหรือไม่ หรือ (ข) การติดตามตรวจสอบพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในสหภาพยุโรป
สหรัฐอเมริกา	● กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกาใช้บังคับเฉพาะกับนิติบุคคลหรือบุคคลซึ่งอยู่ภายใต้เขตอำนาจศาลของสหรัฐอเมริกาเพราะเป็นข้อจำกัดตามรัฐธรรมนูญในเรื่องกระบวนการอันควรแห่งกฎหมาย (Due process)
ออสเตรเลีย	● พระราชบัญญัติความเป็นส่วนตัว ค.ศ. 1988 (Privacy Act 1988) แก้ไขเพิ่มเติมโดยพระราชบัญญัติการแก้ไขความเป็นส่วนตัว (เพิ่มการคุ้มครองความเป็นส่วนตัว) ค.ศ. 2012 (Privacy Amendment (Enhancing Privacy Protection) Act 2012) ใช้บังคับกับการกระทำหรือการปฏิบัติ (act or practice) นอกรัฐและดินแดนของประเทศออสเตรเลียของหน่วยงานภาครัฐและองค์กรภาคเอกชนหรือธุรกิจขนาดเล็กที่มีความเกี่ยวพันกับประเทศออสเตรเลีย (Australian link) เช่น กิจการต่างประเทศที่มีเว็บไซต์มุ่งเสนอขายสินค้าหรือบริการมายังบุคคลในออสเตรเลีย (Office of Australian Information Commissioner, 2014, B.14)
สิงคโปร์	● รัฐบัญญัติคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ ค.ศ. 2012 (Personal Data Protection Act of 2012) มาตรา 2 และมาตรา 3 กำหนดให้ใช้บังคับรัฐบัญญัตินี้กับการเก็บรวบรวม การใช้และการเปิดเผยข้อมูลส่วนบุคคลโดยองค์กร (Organization) (ซึ่งหมายถึงบุคคล บริษัท สมาคมหรือกลุ่มบุคคล ทั้งจดทะเบียนและไม่จดทะเบียน แสวงหากำไรหรือไม่ ไม่ว่าจะจัดตั้งในรูปแบบหรือเป็นที่ยอมรับภายใต้กฎหมายของประเทศสิงคโปร์ ไม่ว่าจะมีถิ่นที่อยู่หรือมีสำนักงานหรือสถานที่ประกอบธุรกิจในสิงคโปร์หรือไม่)
มาเลเซีย	● พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2010 (Malaysia Personal Data Protection Act 2010) มาตรา 2(2)(b) และมาตรา 3 กำหนดให้ใช้พระราชบัญญัตินี้บังคับกับบุคคลที่ไม่ได้อยู่ในประเทศมาเลเซีย แต่ใช้อุปกรณ์ในประเทศมาเลเซียในการประมวลผลข้อมูลส่วนบุคคลนอกเหนือจากการส่งข้อมูลผ่านประเทศมาเลเซีย และใช้บังคับกับบุคคลที่ไม่ได้อยู่ในประเทศมาเลเซีย แต่ได้แต่งตั้งตัวแทนในประเทศมาเลเซียเพื่อวัตถุประสงค์ตามพระราชบัญญัตินี้

ฟิลิปปินส์	● รัฐบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. 2012 (Data Privacy Act of 2012) มาตรา 6 กำหนดหลักการขยายหลักดินแดน (Extraterritorial application) โดยให้ใช้กับการกระทำหรือการปฏิบัติในและนอกฟิลิปปินส์โดยนิติบุคคล ถ้า 1) การกระทำ การปฏิบัติ หรือการประมวลผลเกี่ยวข้องกับข้อมูลส่วนบุคคลของพลเมืองฟิลิปปินส์หรือบุคคลที่มีถิ่นที่อยู่ในประเทศฟิลิปปินส์ 2) นิติบุคคลมีการเชื่อมโยงกับประเทศฟิลิปปินส์และนิติบุคคลมีการประมวลผลข้อมูลส่วนบุคคลในประเทศฟิลิปปินส์ หรือแม้การประมวลผลนอกประเทศฟิลิปปินส์ แต่เป็นการประมวลผลข้อมูลส่วนบุคคลของพลเมืองฟิลิปปินส์หรือผู้มีถิ่นที่อยู่ในประเทศฟิลิปปินส์ รวมถึง (1) สัญญาทำขึ้นในประเทศฟิลิปปินส์ (2) นิติบุคคลไม่ได้จัดตั้งขึ้นในประเทศฟิลิปปินส์ แต่มีการจัดการและการควบคุมหลักในประเทศฟิลิปปินส์ และ (3) นิติบุคคลมีสาขา ตัวแทน สำนักงาน หรือบริษัทย่อยในประเทศฟิลิปปินส์และบริษัทแม่หรือบริษัทในเครือของนิติบุคคลฟิลิปปินส์มีการเข้าถึงข้อมูลส่วนบุคคล และ 3) นิติบุคคลที่มีการเชื่อมโยงอื่น ๆ ในประเทศฟิลิปปินส์ ตัวอย่างเช่น (1) นิติบุคคลประกอบธุรกิจในประเทศฟิลิปปินส์ และ (2) ข้อมูลส่วนบุคคลถูกเก็บรวบรวมหรือจัดเก็บโดยนิติบุคคลในประเทศฟิลิปปินส์
ไทย	● ร่างกฎหมายใช้เฉพาะการเก็บรวบรวม การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยเท่านั้น

3) ประเด็นย่อยที่เกี่ยวข้อง

ประเด็นย่อยที่เกี่ยวข้อง	สหภาพยุโรป	สหรัฐอเมริกา	ออสเตรเลีย	สิงคโปร์	มาเลเซีย	ฟิลิปปินส์	ร่างกฎหมายไทย
1) คำนิยาม “ผู้ควบคุมข้อมูล” และ “ผู้ประมวลผลข้อมูล”	มีคำนิยามทั้งสองคำ	ไม่มีคำนิยามทั้งสองคำ	มีคำนิยามเฉพาะผู้ควบคุมข้อมูล	มีนิยามทั้งสองคำ	มีคำนิยามทั้งสองคำ	มีคำนิยามทั้งสองคำ	มีคำนิยามเฉพาะผู้ควบคุมข้อมูล
2) หน้าที่ผู้ประมวลผลข้อมูล	กำหนดหน้าที่ชัดเจน	ไม่มีการกำหนดหน้าที่ไว้	ไม่มีการกำหนดหน้าที่ไว้	กำหนดหน้าที่ชัดเจน	กำหนดหน้าที่ชัดเจน	กำหนดหน้าที่ชัดเจน	ไม่มีการกำหนดหน้าที่ไว้
3) การโอนข้อมูลออกนอกประเทศ	มีกฎเกณฑ์ชัดเจน	ไม่มีกฎเกณฑ์การโอน	มีกฎเกณฑ์ชัดเจน	มีกฎเกณฑ์ชัดเจน	มีกฎเกณฑ์ชัดเจน	มีกฎเกณฑ์ชัดเจน	มีกฎเกณฑ์บางส่วน

3. การศึกษาปัญหาและอุปสรรคเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ในประเทศไทย

3.1 การศึกษาจากการสัมภาษณ์เชิงลึกกลุ่มผู้เชี่ยวชาญที่เกี่ยวข้อง

ในการสัมภาษณ์เชิงลึกกลุ่มบุคคลที่เกี่ยวข้องกับคลาวด์และการคุ้มครองข้อมูลส่วนบุคคล 10 ท่านทั้งที่เป็นผู้เชี่ยวชาญทางเทคโนโลยีและกฎหมาย ได้รับคำตอบโดยสรุป ดังนี้

1) ผู้เชี่ยวชาญเห็นว่ามาตรการทางเทคนิคที่ใช้ในการรักษาความมั่นคงปลอดภัยของข้อมูลในระบบคลาวด์มีความปลอดภัยเพียงพอหรือไม่ ขึ้นอยู่กับเทคโนโลยีที่นำมาใช้ว่า ทันสมัยกับภัยคุกคามหรือไม่ โดยไม่ว่าจะเป็น public cloud, private cloud หรือ hybrid cloud ความปลอดภัยขึ้นอยู่กับมาตรการทางเทคนิคที่ใช้ในการรักษาความปลอดภัยว่า ทันสมัยกับภัยคุกคามในขณะนั้นหรือไม่ งบประมาณและบุคลากรในการพัฒนาระบบความปลอดภัยเป็นสิ่งสำคัญ (ภูมิ ภูมิรัตน, สัมภาษณ์, 26 กันยายน พ.ศ. 2560)

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) เป็นผู้มีหน้าที่รับผิดชอบพัฒนาระบบคลาวด์ภาครัฐ (Government Cloud : G-Cloud) ซึ่งผ่านการรับรองมาตรฐานด้านความปลอดภัยสารสนเทศ ISO 27001 นอกจากนี้ สรอ. ยังได้รับรางวัล STAR Self-Assessment จาก Cloud Security Alliance (CSA) ข้อมูลส่วนบุคคลที่จัดเก็บในคลาวด์ภาครัฐได้รับความคุ้มครองตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ปัจจุบัน สรอ. มีแนวคิดจัดทำกรอบธรรมาภิบาลข้อมูล (data governance framework) ซึ่งจะมีการจำแนกประเภทข้อมูล (data classification) ที่ชัดเจน เกิดมาตรฐานที่จำเป็น มีนโยบายการใช้งานที่เหมาะสมตามประเภท จนถึงการตรวจสอบความถูกต้องของข้อมูล (ศักดิ์ เสกขุนทด, สัมภาษณ์, 18 ธันวาคม พ.ศ. 2560)

2) ผู้เชี่ยวชาญเห็นว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยควรขยายขอบเขตการบังคับใช้กฎหมายแก่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (เช่น ผู้ให้บริการคลาวด์ เป็นต้น) ที่อยู่นอกประเทศไทย แต่ได้จัดเก็บข้อมูลส่วนบุคคลหรือประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลในไทย เพราะเทคโนโลยีคลาวด์ไร้พรมแดน ข้อมูลส่วนบุคคลอาจถูกเก็บรวบรวม ใช้หรือเปิดเผยที่ใดก็ได้ในโลก (ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล, สัมภาษณ์, 10 สิงหาคม พ.ศ. 2560) แต่ตั้งคำถามเกี่ยวกับสภาพบังคับว่าจะบังคับใช้กฎหมายนอกราชอาณาจักรได้อย่างไร (โกเมน พิบูลย์โรจน์, สัมภาษณ์, 21 กันยายน พ.ศ. 2560)

3) ผู้เชี่ยวชาญเห็นว่าควรแยกนิยาม “ผู้ควบคุมข้อมูลส่วนบุคคล” ออกจาก “ผู้ประมวลผลข้อมูลส่วนบุคคล” เพื่อกำหนดหน้าที่และความรับผิดชอบของแต่ละบุคคลที่ทำงานกับข้อมูลชุดเดียวกันให้ชัดเจน (ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล, สัมภาษณ์, 10 สิงหาคม พ.ศ. 2560 และอาทิตย์ สุริยะวงศ์กุล, สัมภาษณ์, 19 พฤศจิกายน พ.ศ. 2560) นอกจากนี้หลักเกณฑ์สำคัญในการส่งหรือโอนข้อมูลส่วนบุคคลออกนอกราชอาณาจักรไทยควรจะอยู่ในพระราชบัญญัติ ไม่ควรกำหนดไว้ในกฎกระทรวงเพราะจะไม่ถูกตรวจสอบโดยรัฐสภา (อาทิตย์ สุริยะวงศ์กุล, สัมภาษณ์, 19 พฤศจิกายน พ.ศ. 2560)

3.2 การศึกษาจากการสนทนากลุ่มในภาคราชการ ภาคเอกชน ภาควิชาการ และภาคประชาสังคม

ในการสนทนากลุ่ม ผู้เข้าร่วมสนทนากลุ่มได้ให้ความคิดเห็นไว้ ดังนี้

1) นโยบายคลาวด์กับความมั่นคงปลอดภัยในระบบคลาวด์

ปัจจุบัน สรอ. ได้มีการให้บริการคลาวด์ภาครัฐแก่หน่วยงานภาครัฐในระดับกระทรวงทุกกระทรวงแล้ว คลาวด์ภาครัฐของไทยมีมาตรฐานการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากล แต่อุปสรรคในการให้บริการคลาวด์ภาครัฐ ได้แก่ ความ

ล่าช้าในการให้บริการ เนื่องจาก สรอ. ต้องมีการจัดตั้งงบประมาณตามคำขอของหน่วยงานที่ต้องการใช้บริการคลาวด์ภาครัฐแบบปีต่อปี ซึ่งทำให้หน่วยงานภาครัฐที่ต้องการใช้บริการคลาวด์ต้องรอรับบริการในช่วงการจัดสรรงบประมาณซึ่งอาจใช้เวลานานหลายเดือน (ไอรดา เหลืองวิไล, สนทนากลุ่ม, 13 ธันวาคม พ.ศ. 2560)

2) กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับการขยายขอบเขตบังคับใช้กฎหมาย

ธุรกิจขนาดใหญ่ที่ทำธุรกิกับสหภาพยุโรป เช่น ธุรกิจสายการบิน ธุรกิจโรงแรม ธุรกิจท่องเที่ยว เป็นต้น มีความเสี่ยงทางกฎหมายที่ต้องตกอยู่ภายใต้การขยายหลักดินแดนกาคุ้มครองข้อมูลส่วนบุคคลของกฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หากธุรกิจเหล่านี้ได้เก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลในสหภาพยุโรปผ่านสื่อออนไลน์ เช่น การขายตั๋วเครื่องบินให้บุคคลในสหภาพยุโรปผ่านเว็บไซต์ เป็นต้น ผู้เชี่ยวชาญท่านหนึ่งมีความเห็นว่า การบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลในไทยมีผลดีต่อธุรกิจของตนเพราะจะได้มีหลักเกณฑ์ชัดเจนในการปฏิบัติตามกฎหมาย (สิทธินัย จันทรานนท์, สนทนากลุ่ม, 13 ธันวาคม พ.ศ. 2560) แต่ผู้เชี่ยวชาญอีกท่านหนึ่งเห็นว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลอาจเป็นการเพิ่มภาระกับผู้ประกอบธุรกิจขนาดกลางและขนาดย่อมที่ไม่มีความพร้อมในการปฏิบัติตามกฎหมาย (เกรียงศักดิ์ สวัสดิ์พาณิชย์, สนทนากลุ่ม, 13 ธันวาคม พ.ศ. 2560) โดยผู้เชี่ยวชาญหลายท่านที่เข้าร่วมสนทนากลุ่มมีความเห็นว่าร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลต้องเพิ่มบทบัญญัติเกี่ยวกับขอบเขตการบังคับใช้กฎหมายแก่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกประเทศไทยไว้ ทั้งนี้เพราะปัจจุบันธุรกิจในประเทศไทยมีการใช้ระบบคลาวด์ที่อยู่นอกประเทศไทยในการจัดเก็บข้อมูลส่วนบุคคลเป็นจำนวนมาก หากไม่มีการขยายขอบเขตการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล ในกรณีเกิดการละเมิดข้อมูลส่วนบุคคล ธุรกิจที่เป็นผู้ควบคุมข้อมูลในไทยอาจต้องรับผิดตามกฎหมายโดยลำพัง โดยไม่อาจไปไล่เบี้ยเอากับผู้ประมวลผลข้อมูลส่วนบุคคล (ผู้ให้บริการคลาวด์) นอกประเทศได้ เพราะภายใต้ข้อตกลง (clauses) ในสัญญาให้บริการคลาวด์ส่วนใหญ่มักมีข้อยกเว้นจำกัดความรับผิดของผู้ให้บริการไว้ในสัญญา ฉะนั้นการกำหนดบทบัญญัติเกี่ยวกับการขยายขอบเขตการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลไว้ จะทำให้ผู้ประมวลผลข้อมูลส่วนบุคคล (ผู้ให้บริการคลาวด์) ที่อยู่นอกประเทศไทยยังต้องรับผิดตามกฎหมายไทย (ภูมิ ภูมิรัตน, สนทนากลุ่ม, 13 ธันวาคม พ.ศ. 2560 และวรรณวิทย์ อาขุบุตร, สนทนากลุ่ม, 13 ธันวาคม พ.ศ. 2560)

3) ประเด็นย่อยที่เกี่ยวข้อง

(1) ความหมายของ “ผู้ควบคุมข้อมูลส่วนบุคคล” และ “ผู้ประมวลผลข้อมูลส่วนบุคคล” ต้องมีนิยามให้ชัดเจนและกำหนดหน้าที่ให้เหมาะสม (ภูมิ ภูมิรัตน, สนทนากลุ่ม, 13 ธันวาคม พ.ศ. 2560) ในบางกรณีบุคคลหรือนิติบุคคลหนึ่ง ๆ อาจเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลก็ได้ ทั้งนี้ขึ้นอยู่กับหน้าที่ความรับผิดชอบที่ได้กระทำต่อข้อมูล เช่น กูเกิล (Google) อาจเป็นผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่เป็นผู้เก็บรวบรวมข้อมูลในเว็บไซต์สืบค้นข้อมูล (search engine) แต่อาจถือว่า เป็นผู้ประมวลผลข้อมูลส่วนบุคคลในกรณีที่เป็นผู้ให้บริการกูเกิลคลาวด์ (Google Cloud) (อาทิตย์ สุริยะวงศ์กุล, สนทนา

กลุ่ม, 13 ธันวาคม พ.ศ. 2560) เป็นต้น

(2) การเก็บรวบรวมข้อมูลในระบบคลาวด์มีลักษณะเป็นการส่งหรือโอนข้อมูลออกไปยังต่างประเทศโดยสภาพ เพราะผู้ให้บริการคลาวด์ต่างประเทศมักมีดาต้าเซ็นเตอร์อยู่ในต่างประเทศ (วรรณวิทย์ อาขุบุตร, สนทนากลุ่ม, 10 มกราคม พ.ศ. 2561) ดังนั้น ทันทีที่มีการเก็บรวบรวมข้อมูล ข้อมูลดังกล่าวก็จะถูกส่งหรือโอนไปยังดาต้าเซ็นเตอร์ที่อยู่ต่างประเทศโดยอัตโนมัติ โดยเฉพาะในธุรกิจสายการบิน การส่งหรือโอนข้อมูลส่วนบุคคลข้ามพรมแดนเกิดขึ้นตลอดเวลา การห้ามหรือจำกัดการส่งหรือโอนข้อมูลส่วนบุคคลข้ามพรมแดนจึงส่งผลกระทบต่อธุรกิจอย่างแน่นอน ด้วยเหตุนี้ หลักเกณฑ์ในการส่งหรือโอนข้อมูลส่วนบุคคลข้ามพรมแดนระหว่างประเทศจึงจำต้องมีความชัดเจนแน่นอน (สิทธินัย จันทรานนท์, สนทนากลุ่ม, 10 มกราคม พ.ศ. 2561)

อภิปรายและสรุปผลการวิจัย

จากการศึกษาข้อมูลเอกสารที่ได้จากการเปรียบเทียบนโยบายคลาวด์และการคุ้มครองข้อมูลส่วนบุคคลระหว่างสหภาพยุโรป สหรัฐอเมริกา ออสเตรเลีย สิงคโปร์ มาเลเซีย ฟิลิปปินส์ และไทย (ข้อ 4.1) รวมถึงการสัมภาษณ์เชิงลึกกลุ่มผู้เชี่ยวชาญที่เกี่ยวข้อง (ข้อ 4.2) และการรับฟังความเห็นจากผู้เข้าร่วมสนทนากลุ่ม (ข้อ 4.3) สามารถสรุปและวิเคราะห์ผลการศึกษาได้โดยแบ่งเป็น 2 ประเด็นหลัก ดังนี้

1) นโยบายคลาวด์กับความมั่นคงปลอดภัยในระบบคลาวด์

การจัดเก็บข้อมูลรวมไว้ในคลาวด์มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง นโยบายของรัฐบาลมีส่วนสำคัญในการสนับสนุนการใช้งานคลาวด์ สหภาพยุโรป สหรัฐอเมริกา ออสเตรเลีย สิงคโปร์ มาเลเซีย และฟิลิปปินส์ต่างให้การสนับสนุนการใช้งานคลาวด์โดยการประกาศนโยบายคลาวด์ที่ชัดเจน สำหรับประเทศไทยคือ สรอ. มีบทบาทสำคัญในการผลักดันการใช้คลาวด์ภาครัฐ และได้กำหนดมาตรฐานการรักษาความปลอดภัยด้านสารสนเทศตามมาตรฐานสากล แต่อุปสรรคสำคัญในการให้บริการคลาวด์ภาครัฐของไทยคือ ความล่าช้าในการให้บริการเนื่องจาก สรอ. ต้องจัดตั้งงบประมาณให้หน่วยงานตามคำขอของหน่วยงานของรัฐที่ต้องการใช้บริการปีต่อปี ดังนั้น จึงจำเป็นต้องมีการปรับปรุงขั้นตอนการจัดสรรงบประมาณภาครัฐเกี่ยวกับการขอใช้บริการคลาวด์ภาครัฐ เพื่อให้เกิดความรวดเร็วยิ่งขึ้น

อย่างไรก็ดี การใช้งานคลาวด์มีความมั่นคงปลอดภัยไม่แตกต่างกับการสร้างดาต้าเซ็นเตอร์ขึ้นจัดเก็บข้อมูลเอง ทั้งนี้ขึ้นอยู่กับบุคลากรที่ดูแลโครงสร้างพื้นฐาน (infrastructure) และงบประมาณในการออกแบบระบบความปลอดภัย ประเด็นจึงอยู่ที่การบริหารความเสี่ยงของข้อมูล (data risk management) การจัดทำกรอบธรรมาภิบาลข้อมูล (data governance framework) และการจำแนกประเภทข้อมูล (data classification) เพื่อการจัดการและใช้ข้อมูลอย่างเหมาะสม จะเป็นการยกระดับการรักษาความมั่นคงปลอดภัยของข้อมูลที่จัดเก็บไว้ในระบบคลาวด์ของไทย

2) กฎหมายคุ้มครองข้อมูลส่วนบุคคลกับการขยายขอบเขตการบังคับใช้กฎหมาย

(1) กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ประเทศในกลุ่มโออีซีดี (OECD) 35 ประเทศ กลุ่มเอเปก 21 เขตเศรษฐกิจ (20 ประเทศกับ 1 เขตปกครองพิเศษ) และสหภาพยุโรป 28 ประเทศ มีเพียง 6 ประเทศในกลุ่มเอเปกคือ

ชิลี อินโดนีเซีย ปาปัวนิวกินี เวียดนาม บรูไน และไทยที่ไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล แม้ปัจจุบันไทยมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเฉพาะเรื่อง เช่น พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 หรือพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 เป็นต้น แต่ยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของคนไทยที่ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยธุรกิจเอกชนเป็นการทั่วไป ข้อมูลส่วนบุคคลซึ่งจัดเก็บในระบบคลาวด์ถือว่า เป็นข้อมูลทางการตลาดที่สำคัญที่สามารถเคลื่อนย้ายข้ามพรมแดนได้โดยง่าย การออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลจึงเป็นการจำเป็นอย่างยิ่งในการคุ้มครองข้อมูลส่วนบุคคลของคนในประเทศจากการเก็บรวบรวม ใช้หรือเปิดเผยโดยไม่ชอบทั้งจากธุรกิจภายในและภายนอกประเทศ อย่างไรก็ดี ธุรกิจขนาดกลางและขนาดย่อมตามพระราชบัญญัติส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม พ.ศ. 2543 อาจยังไม่พร้อมปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ในกรณีดังกล่าว กฎหมายอาจกำหนดเวลาให้ธุรกิจเหล่านี้ต้องปฏิบัติตามกฎหมายเมื่อพ้นระยะเวลา 3 ปี นับแต่วันที่กฎหมายนี้บังคับใช้ เพื่อให้มีเวลาในการเตรียมความพร้อมก็ได้

(2) **ผลของการขยายหลักดินแดนคุ้มครองข้อมูลส่วนบุคคลของกฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่มีต่อธุรกิจไทย**

เมื่อกฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปมีผลบังคับใช้ ธุรกิจในประเทศไทยที่เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลส่วนบุคคลในสหภาพยุโรป (โดยไม่ต้องคำนึงถึงว่าการชำระเงินของเจ้าของข้อมูลส่วนบุคคลดังกล่าวจะเกิดขึ้นในสหภาพยุโรปหรือไม่) หรือการติดตามตรวจสอบพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในสหภาพยุโรป ตัวอย่างเช่น ธุรกิจสายการบินในไทยที่มีการขายตั๋วเครื่องบินให้แก่ผู้โดยสารที่อยู่ในสหภาพยุโรปและมีการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้โดยสารดังกล่าว หรือธุรกิจโรงแรมในไทยที่มีการขายห้องพักให้แก่นักท่องเที่ยวที่อยู่ในสหภาพยุโรปผ่านทางเว็บไซต์ต่าง ๆ ไม่ว่าจะเป็นเว็บไซต์ของโรงแรมเองหรือเว็บไซต์ของตัวแทนแล้วมีการเก็บรวบรวมข้อมูลส่วนบุคคลของนักท่องเที่ยวดังกล่าว หรือธุรกิจโรงพยาบาลในไทยที่มีผู้ป่วยเป็นบุคคลในสหภาพยุโรปแล้วมีการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้ป่วยคนนั้นในสหภาพยุโรปเพื่อการวิเคราะห์วินิจฉัยโรคในประเทศไทย หรือบริษัทท่องเที่ยวในไทยที่มีลูกค้านักท่องเที่ยวจากสหภาพยุโรปโดยมีการเก็บรวบรวมข้อมูลส่วนบุคคลของนักท่องเที่ยวคนนั้นในสหภาพยุโรปเพื่อการให้บริการในประเทศไทย รวมธุรกิจอีคอมเมิร์สในไทยทั้งหมดที่ขายสินค้าหรือให้บริการแก่ลูกค้าในสหภาพยุโรปโดยมีการเก็บข้อมูลส่วนบุคคลของลูกค้าคนนั้นในสหภาพยุโรป ตลอดจนผู้ให้บริการคลาวด์หรือดาต้าเซ็นเตอร์ในไทยที่ให้บริการประมวลผลข้อมูลหรือจัดเก็บข้อมูลส่วนบุคคลของเจ้าของข้อมูลในสหภาพยุโรป ต้องตกอยู่ภายใต้กฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปทั้งสิ้น ธุรกิจเหล่านี้ต้องเข้าใจถึงความเสี่ยงทางกฎหมายที่อาจเกิดขึ้นจากการละเมิดข้อมูลส่วนบุคคลของบุคคลในสหภาพยุโรปที่อยู่ในการจัดเก็บของตน โดยจะต้องกำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคลขององค์กรที่สอดคล้องกับกฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป โดยต้องปฏิบัติตามนโยบายดังกล่าวอย่างเคร่งครัด

(3) การขยายขอบเขตบังคับใช้กฎหมายแก่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกประเทศไทยซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลภายในประเทศไทย

ปัจจุบัน เทคโนโลยีคลาวด์ทำให้การประมวลผลข้อมูลส่วนบุคคลสามารถกระทำได้โดยไร้พรมแดน ข้อมูลส่วนบุคคลของคนไทยในประเทศไทยอาจถูกเก็บรวบรวม ใช้ หรือเปิดเผยผ่านเครือข่ายอินเทอร์เน็ตจากธุรกิจในต่างประเทศโดยดาต้าเซ็นเตอร์ซึ่งตั้งอยู่ที่ใดในโลกก็ได้ กฎหมายที่ใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลเฉพาะที่อยู่ในราชอาณาจักรไม่สามารถนำมาปรับใช้ได้อย่างมีประสิทธิภาพกับเทคโนโลยีคลาวด์และอินเทอร์เน็ต ฉะนั้น การขยายขอบเขตบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกประเทศ แต่ได้ทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลภายในประเทศไทยจึงเป็นวิธีการหนึ่งที่สามารถเพิ่มประสิทธิภาพของกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของคนไทยในประเทศไทย แม้การบังคับใช้กฎหมายอาจกระทำได้ยากเพราะบุคคลดังกล่าวอยู่นอกเขตอำนาจศาลไทย แต่การบัญญัติกฎหมายลักษณะนี้ถือว่า เป็นการส่งสัญญาณการคุ้มครองข้อมูลส่วนบุคคลของคนไทยในประเทศให้แก่บุคคลที่อยู่นอกประเทศไทยให้ตระหนักว่า หากประสงค์จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของคนไทยในประเทศไทย ธุรกิจนั้นต้องให้ความคุ้มครองข้อมูลส่วนบุคคลของคนไทยในประเทศไทยตามมาตรฐานของกฎหมายไทย ดังนั้น งานวิจัยนี้จึงเสนอให้เพิ่มบทบัญญัติขยายขอบเขตการบังคับใช้กฎหมายแก่ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกประเทศไทย โดยมีเนื้อหาดังนี้ “พระราชบัญญัตินี้ให้ใช้บังคับกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักรโดยผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลทั้งที่อยู่ในราชอาณาจักรและนอกราชอาณาจักร”

3) ประเด็นย่อยที่เกี่ยวข้อง

คำว่า “ผู้ประมวลผลข้อมูลส่วนบุคคล” ไม่ปรากฏในร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.... (ฉบับที่คณะกรรมการกฤษฎีกาตรวจพิจารณาแล้ว เรื่องเสร็จที่ 1135/2558) จึงจำต้องบัญญัติเพิ่มเติม โดยอาจนำความหมายตามกฎข้อบังคับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปมาเป็นต้นแบบในการร่างว่าหมายถึง “บุคคลหรือนิติบุคคล หรือหน่วยงานภาครัฐ หรือองค์กรอื่นใด ทั้งจดทะเบียนและไม่จดทะเบียน โดยลำพังหรือร่วมกัน และไม่ว่าจะมีถิ่นที่อยู่หรือมีสำนักงานหรือสถานที่ประกอบการในไทยหรือไม่ ที่ประมวลผลข้อมูลส่วนบุคคลแทนหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล” และควรกำหนดหน้าที่ผู้ประมวลผลข้อมูลส่วนบุคคลไว้เป็นการเฉพาะอย่างน้อย 4 ประการ ดังนี้

(1) หน้าที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งโดยชอบด้วยกฎหมายที่เป็นลายลักษณ์อักษรของผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น

(2) หน้าที่รักษาความปลอดภัยของข้อมูลโดยใช้มาตรการในการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม

(3) หน้าที่แจ้งผู้ควบคุมข้อมูลส่วนบุคคลให้ทราบถึงการละเมิดข้อมูลส่วนบุคคลโดยไม่ชักช้า และ

(4) หน้าที่ปฏิบัติตามหลักเกณฑ์การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

นอกจากนี้ การเก็บรวบรวมข้อมูลส่วนบุคคลของคนไทยในประเทศไทยในระบบคลาวด์ของบริษัทในต่างประเทศ มักเป็นการส่งหรือโอนข้อมูลออกนอกประเทศไทยโดยสภาพ ดังนั้น หลักเกณฑ์ในการส่งหรือโอนข้อมูลดังกล่าวไปต่างประเทศจึงต้องมีความชัดเจนและเพียงพอต่อการรักษาความปลอดภัยของข้อมูล ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยจึงควรกำหนดหน้าที่ของผู้ส่งหรือโอนข้อมูลส่วนบุคคลในการรักษาความมั่นคงปลอดภัยของข้อมูลไว้ว่า “ห้ามมิให้บุคคลหรือนิติบุคคลใดส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศหรือดินแดนนอกประเทศไทย เว้นแต่ประเทศผู้รับข้อมูลส่วนบุคคลมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่คล้ายคลึงกับประเทศไทย หรือบุคคลหรือนิติบุคคลที่ส่งหรือโอนข้อมูลส่วนบุคคลนั้น ได้จัดให้มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลส่วนบุคคลเทียบเท่าที่กำหนดไว้ในพระราชบัญญัตินี้”

กิตติกรรมประกาศ

โครงการวิจัยนี้ได้รับทุนอุดหนุนจากสำนักงานคณะกรรมการวิจัยแห่งชาติ (วช.) และสำนักงานกองทุนสนับสนุนการวิจัย (สกว.) และความเห็นในรายงานผลการวิจัยเป็นของผู้วิจัย สำนักงานคณะกรรมการวิจัยแห่งชาติ (วช.) และสำนักงานกองทุนสนับสนุนการวิจัย (สกว.) ไม่จำเป็นต้องเห็นด้วยเสมอไป

References

Allen & Overy. (2017). The EU Data Protection Regulation. Retrieved from http://www. allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

Asia Cloud Computing Association. (2016). Cloud Readiness Index 2016. Retrieved from http://www.asiacloudcomputing.org/research/2016-research/cri2016

Australian Government, Department of Finance. (2014). Australian Government Cloud Computing Policy, Smarter ICT Investment. Version 3.0. Retrieved from https://www.dta.gov.au/files/Australian%20Government%20Cloud%20Computing%20Policy%203.0-WCAG.pdf

DLA PIPER. (2018). Data Protection Laws of the World. Retrieved from https://www.dlapiperdataprotection.com

European Commission. (2015). A Digital Single Market Strategy for Europe. COM 192 final.

Gartner Inc. (2017). Gartner Says Worldwide Public Cloud Services Market to Grow 18 Percent in 2017. Newsroom, Press Release, Stamford, Conn. Retrieved from http://www.gartner.com/newsroom/id/3616417

Infocomm Media Development Authority of Singapore. (2017). Multi Tier Cloud Security Certified Cloud Services. Retrieved from https://www.imda.gov.sg/industry-development/infrastructure/ict-standards-and-frameworks/mtcs-certification-scheme/multi-tier-cloud-security-certified-cloud-services

Malaysia Digital Economic Corporation. (2017). Building Malaysia's Digital Future. Retrieved from https://mdec.my/about-mdec

Office of Australian Information Commissioner. (2014). Australian Privacy Principles guidelines, Privacy Act 1988. Retrieved from https://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP-guidelines-combined-set-v1.pdf

Republic of Philippines, Department of Information and Communications Technology. (2017). Prescribing the Philippine Government's Cloud First Policy, (Department Circular No.2017-002) Retrieved from http://www.dict.gov.ph/wp-content/uploads/2017/02/Signed_DICT-Circular_2017-002_CloudComp_2017Feb07.pdf

Sainul, A. K. (2017). Malaysia to Introduce 'Cloud First' Strategy, to Develop a National AI Framework. Retrieved from https://e27.co/malaysia-introduce-cloud-first-strategy-develop-national-ai-framework-20171020

Samuel, D. W., Louis, D. B. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193-220.

Segkhoonthod, S. (2017). Data Governance is Urgently Required in the Management and Use of Data. Retrieved from https://www.ega.or.th/th/content/890/12248 (in Thai)

U.S. Government's National Institute of Standards and Technology (NIST). (2001). Definition of Cloud Computing, (Special Publication 800-145).

Vivek, K. (2011). Federal Cloud Computing Strategy. The White House, Washington.